Fraud Prevention

CREDIT UNION 1

Never Give Out Information When a Company Reaches Out to You

Treat every e-mail, text and phone call as an opportunity to call the company back or to log in to their website. A real company will never ask you to send personal information over email or text. If the communication is legitimate, it will come through the US Postal Service in an official envelope or it will be displayed on their website once you log in. If you call the company back, always look up their phone number on their website (make sure to verify it is their authentic site).

Don't Click That Link

Even if a company you know and trust sends you an email, be careful and make sure it's legitimate before you click on any of the included links. Scammers, known as Phishers, masquerade as real businesses and try to get you to plug in personal information to their fake websites. Don't fall for it - always go straight to the company's website from your browser using the URL or your bookmarks.

Safeguard Your Social Security Number

Only give out your social security number when absolutely necessary. Most of the time you can use your driver's license or other form of photo ID for identification. Just make sure you know how this personal information is going to be used and if it will be shared.

Shred the Paper

This includes junk mail, statements, bills and checks. Many identity theft cases are linked to paper mail. Make sure you securely destroy everything with personal information on it. Better yet, stop it completely by signing up for paperless options.

Stop the Paper

Sign up for e-Statements and get your Credit Union 1 statements and other communications sent electronically. Stop those credit card offers by opting out of direct mailing lists, and get yourself on the national Do Not Call registry to stop telemarketers.

Common Scams

Work-from-home job offers, secret shopping and winning the lottery you never bought a ticket for are all common scams. If something sounds too good to be true, look for it on the Federal Trade Commission's Scam Alerts at: http://www.consumer.ftc.gov/

Buyer Beware

When using a credit card online make sure the URL reads "https://". The "s" means it's a secure site. When buying or selling something online, always deal locally with people you can meet (safely) in person. Steer clear of anyone using Western Union, MoneyGram, or other wire services. Never cash a check (even a Cashier's Check) and give the buyer money back – this is always a scam. For more info on safe online buying and selling check out: https://www.fbi.gov/scams-safety/fraud/internet_fraud